

REMARKS

This Request for Reconsideration after Final is filed in response to a Final Office Action of January 22, 2010 in which claims 129-182 were rejected.

In the "Response to Arguments" Section on pages 2-4, the Examiner found practically all Applicant's arguments not persuasive. The Applicant respectfully disagrees and in turn is of opinion that many arguments presented by the Examiner are inaccurate and unsubstantiated. The purpose of this submission is to reiterate and summarize one more time major points of disagreement and to convince the Examiner to allow the case.

Claim Rejections - 35 USC § 112**Examiner's Position:**

Claims 136, 159 and 172 are rejected under 35 USC 112, first paragraph, as failing to comply with the written description requirement. These claims recite "an index indicating how to enter ... Transmission event unabridged" which is not described in the specification.

Applicant's Response:

The Applicant respectfully disagrees with the Examiner.

In addition to arguments presented in the Request for Reconsideration submitted to the USPTO on October 27, 2010, the Applicant would like to point out that starting on page 6 line 1 through page 6, line 6 of the originally filed patent application, it is stated: "For example, an index may provide an indication of the location of a particular type of notification, By storing and/or indexing data in this manner (i.e., in relatively small data structures), the system may provide for the storage of network event notification data as it is processed in its entirety." From this quote it is apparent to a

person skilled in the art that the index (or indexing) would comprise the indication of the location of the event transmission/notification (whether it is saved partially or in its entirety).

In light of the above citation it is clear to a person skilled in the art how to enter unabridged transmission event (i.e., event notification) using created index (or using "indexing"). In other words, if a notification (transmission event) is saved in its entirety, a characterization record, e.g., an index or an index comprising observation record/records should indicate where this notification is saved. If the Examiner is still not convinced, the Applicant would like to challenge the Examiner to indicate which characterization record then comprise information about location of, e.g., of the unabridged transmission event (after all, some record should indicate such a location whether you call it index or something else).

Claim Rejections - 35 USC § 103

Examiner's Position:

Claims 129-135, 137-140, 142-145, 148-154, 156-158, 160-171, 173-176 and 178-179 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanokar et al. (U.S. Patent No. 6560443) in view of Wiley et al. (US 7382756).

Claims 141, 155 and 177, are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanokar et al. in view of Wiley et al. as applied to claims 129, 148 and 166 and further in view of Richards et al. (US 2005/0015461).

Claims 146, 147, 181 and 182 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanokar et al. as applied to claims 129, 148 and 166 and further in view Microsoft Computer Dictionary, 5th Edition.

Applicant's Response:

The Applicant is of opinion that Examiner's arguments are inaccurate. The Examiner's arguments are analyzed based on MPEP guidelines which are stated in the MPEP Paragraph 2143 as follows:

"To establish a *prima facie* case of obviousness three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicant's disclosure. ***In re Vaeck***, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)."

In reference to independent claim 129 (and other independent claims) of the present patent application, on page 5 of the Final Office Action of October 30 2009, the Examiner admitted that Khanokar et al. did not show all features of a second step in claim 129 but further stated that Wiley et al. disclose the second step of claim 129:

"creating one or more characterization records for at least one data structure of said one or more data structures, one or more transmission events of said plurality of the transmission events being collected to said at least one data structure of said one or more data structures, wherein at least one of said one or more characterization records comprises one or more indicators of a location or locations of one or more data elements comprised in at least one of said one or more

transmission events, to allow accessing said at least one of the one or more characterization records to determine said one or more indicators of the location or locations of said one or more data elements."

The Applicant is of opinion that Wiley et al. did not disclose the above passage from claim 129 of the present patent application, contrary to what is alleged by the Examiner.

Wiley et al. disclosed root and child datasets 50 (54 and 56) shown in Figure 2, such that root datasets having keysets 58 and 60 which include source IP address, source port, destination IP address and/or destination port key combination (see Figure 2 and col. 4 lines 55-57 of Wiley et al.), and pointers 106, 108, 110 and 112 shown in figure 3 of Wiley et al. which may be updated when child and/or sibling databases are created, such that the root datasets can point out to the child or sibling datasets (e.g., see col. 5, lines 22-25, col. 5, lines 53-56, col. 6, lines 11-15, col. 6, lines 27-28 of Wiley et al.).

In order to compare disclosure of Wiley et al. with the subject matter recited in claim 129 of the present patent application, equivalency between the components recited in claim 129 of the present application and in Wiley et al. should be established by the USPTO.

Even though the Final Office Action of January 22, 2010 does not establish such an equivalency, the Applicant's understanding is that the Examiner alleged that the description provided by Wiley et al. may be interpreted in such a way that the pointers of Wiley et al. may be equivalent to "one or more indicators of a location or locations of one or more data elements of one or more data elements comprised in at least one of said one or more transmission events" as recited in claim 129 of the present patent application, i.e., indicators of a location or locations are equivalent to pointers of Wiley et al.

This "established equivalency" by the Applicant was not objected by the Examiner in the Final Office Action of January 22, 2010, even though the burden of proof is on the Office, such that this equivalency should be established by the Office.

Moreover, in regard to rejection of the second step of claim 129, the Applicant's point of view is that the keysets 58 and 60 of Wiley et al. (also see examples of keysets in Figure 4 of Wiley et al.) are not equivalent to "one or more data elements" recited in claim 129 of the present patent application because keysets 58 and 60 are equivalent to data features or characteristics of the corresponding transmission events (as quoted above from col. 4 lines 55-57 of Wiley et al.). Therefore, Wiley et al. do not disclose saving any one or more data elements comprised in at least one of said one or more transmission events as recited in claim 129 because Wiley et al. do not teach saving data elements at all, but only saving features and characteristics of the data elements in corresponding keysets.

It is noted by the Applicant that "information itself" mentioned in col. 4, lines 26-28 Wiley et al. is different that "one or more data elements comprised in at least one of said one or more transmission events" recited in claim 129 because the previous sentence in col. 4, lines 24-26 of Wiley et al. unambiguously clarifies that this term "information itself" is referred to information comprised in the IP Packet which contains "a source IP address, a source port, a destination IP address and a destination port". Therefore, this "information itself" has nothing to do with the "one or more data elements" (i.e., the original data comprised in the transmission event) recited in claim 129 as referenced above.

Moreover, in col. 7 lines 35-51 of Wiley et al. quoted by the Examiner, Wiley et al. discuss dataset/pointers/keyset

operation (e.g., pointing at datasets comprising features and characteristics of the data comprised in keysets) and has nothing to do with pointing at the "one or more data elements" recited in claim 129 (the burden of proof is on the Office).

Thus, nothing in the disclosure of Wiley et al. indicates that any of the originally received transmission event data is saved, which makes sense, because Wiley et al. do not need to save any originally received data since the "problem to be solved" by Wiley et al. is not to get access to the originally received data (which may be one problem solved by the present patent application) but to detect intrusion network activity, and for that purpose, only data representative (in order to generate a "signature") is needed and therefore stored in datasets which include keysets (e.g., see col. 4 lines 18-30 and ABSTRACT of Wiley et al.).

Therefore, none of the references (Khanokar et al. or Wiley et al.) quoted by the Examiner teach or disclose a second step of claim 129 quoted herein, such that none of these references disclose all limitations of claim 129, as required by the MPEP Paragraph 2143 quoted herein, which makes claim 129 non-obvious and not unpatentable over Khanokar et al. in view of Wiley et al. under 35 U.S.C. 103(a), contrary to what is alleged by the Examiner.

But even if we assume for the sake of argument only that Khanokar et al. and Wiley et al. disclose all steps and limitations of claim 129 of the present patent application (which is not the case as shown herein), the Examiner did not show correctly that the quoted references contain suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings to arrive at the subject

matter of claim 129 (and other independent and dependent claims) of the present invention.

Indeed, on page 6 (top paragraph) of the Final Office Action of January 22, 2010, the Examiner stated that "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Khanokar et al. with that of Wiley in order to provide faster access to stored data (Wiley, col. 2, lines 17-28)". The Applicant only partially agrees with the Examiner in a sense that "providing effective access to stored data" is one of the problems solved by the present invention, however, not necessarily providing a faster access, because "faster" is a relative term. In other words someone may ask a question: "faster" relative to what? Also, the Applicant totally disagrees with the Examiner stating that Wiley et al. provide in col. 2, lines 17-28 motivation for combining references of Khanokar et al. and Wiley et al. to reach the stated goal of "providing faster access to stored data". The problem to be solved by both inventions of Khanokar et al. and Wiley et al. is related to providing security (e.g., detecting network intrusion events as evident from ABSTRACTS of both patent applications). Then the Examiner's reference to col. 2 lines 17-28 of Wiley et al. to provide justification for combining references of Khanokar et al. and Wiley et al. is unsupported by the disclosure of Wiley et al. because it is clearly stated in col. 2 lines 17-19 of Wiley et al. that "Technical advantages of the present patent application include providing an improved method and system for maintaining network activity data for intrusion detections." Nothing is indicated in col. 2 lines 17-28 of Wiley et al. about "providing faster access to stored data". The datasets with keysets and pointer system disclosed by Wiley et al. is for creating a signature for

intrusion detection, as discussed herein, and not for "providing faster access to stored data", as alleged by the Examiner.

This further reinforce the conclusion that claim 129 is not unpatentable under 35 U.S.C. 103(a) over Khanokar et al. in view of Wiley et al., as stated herein.

Independent claims 148 and 166 have a similar scope as claim 129 and therefore also not unpatentable over Khanokar et al. in view of Wiley et al. under 35 U.S.C. 103(a).

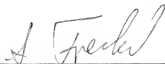
The non-obviousness and patentability of dependent claims 130-147, 149-165 and 187-182 is provided by novelty and non-obviousness of the independent claims 129, 149 and 166 they are dependent from (directly or indirectly). More arguments in reference to unique limitations of dependent claims 130-148, 150-165 and 187-182 may be presented by the applicant if requested by the Office.

CONCLUSION

The objections and rejections of the Final Office Action of October 30, 2009 and of the Advisory Action of January 6, 2010 having been obviated by amendment or shown to be inapplicable, withdrawal thereof is requested and passage of all claims to issue is earnestly solicited.

Respectfully submitted,
KELLEY DRYE & WARREN LLP
Attorneys and Agents for Applicants

Date: February 17, 2010



Anatoly Frenkel
Reg. No. 54,106

400 Atlantic Street
Stamford, CT 06901
Direct Tel.: 203-351-8078
Facsimile: 203-327-2669
e-mail: afrenkel@kelleydrye.com